Rafey S. Balabanian (SBN 315962)
rbalabanian@edelson.com
EDELSON PC
150 California Street, 18th Floor
San Francisco, California 94111
Tel: 415.212.9300
Fax: 415.373.9435

Counsel for Plaintiffs David Melvin, J.L., and the Putative Classes

UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF CALIFORNIA

SAN FRANCISCO DIVISION

DAVID MELVIN and J.L., individually and on behalf of all others similarly situated, *Plaintiffs,* *v.* **23ANDME, INC.**, a Delaware corporation, *Defendant.*	Case No. _____ **CLASS ACTION COMPLAINT FOR:** **(1) Negligence;** **(2) Threat Assessment and Monitoring;** **(3) Violation of Cal. Bus. & Prof. Code § 17200, *et seq.*;** **(4) Violation of 410 ILCS 513, *et seq.*; Alaska Stat. § 18.13.010, *et seq.*; Or. Rev. Stat. § 192.531, *et seq.*; and** **(5) Declaratory Judgment.** **DEMAND FOR JURY TRIAL**

Plaintiffs David Melvin and J.L., on behalf of themselves and all others similarly situated, bring this class action complaint against Defendant 23andMe, Inc. ("23andMe") and allege as follows upon personal knowledge as to themselves and their own acts and experiences, and, as to all other matters, upon information and belief.

INTRODUCTION

1. Genetic data is the "holy grail" of personal information. DNA can be used to reveal an individual's health, explore their family history, and even identify their ethnicity. But genetic data can also be exploited for discriminatory and abusive purposes, from denying

individuals and their families employment opportunities or health and life insurance, to creating "hit lists" of minorities and other vulnerable populations, like what shockingly has happened here.

2. On December 5, 2023, one of the largest direct-to-consumer genetic testing companies, 23andMe, notified 7 million customers that a "threat actor" accessed their accounts without authorization "in early October" through a process called credential stuffing. From the outset, 23andMe appeared to wash its hands of the situation, blaming its customers for reusing passwords from other websites and telling them that it has no "indication that there was a data security incident" within its systems.

3. What 23andMe knew—but concealed—from those 7 million customers was that their private genetic information ("PGI") was leaked on the dark web two months earlier on October 1, 2023, along with their genetic heritage, ancestral origin, full names, home addresses, profile pictures, and birth dates. Discovery will show that 23andMe delayed sending notice of the breach to these 7 million customers so that it could first change its terms and conditions to add onerous arbitration requirements that were specifically aimed at preventing them from pursuing claims against the company.

4. As if this was not bad enough, 23andMe also concealed that Jewish and Chinese customers were specifically targeted by the hacker and that their PGI was compiled into specially curated lists that were shared and sold on the dark web and continue to be shared and sold to this day. Discovery will show that 23andMe reviewed this data and confirmed it was legitimate, but nonetheless concealed this information from its Jewish and Chinese customers.

5. This is not a typical data breach. The hacker leaked the list of over 1 million Jewish customers expressly in retribution for the Israel-Hamas war, and was more than happy to leak the list of 350,000 Chinese customers upon request from a user with the alias "Wuhan." These lists generated a huge amount of interest from hackers on the dark web from all over the world and were shared and reshared an untold number of times.

6. The disclosure of the Jewish and Chinese lists threatens the safety and security of those customers and subjects them to harassment, vandalism, assault, and discrimination.

And given the Chinese government's long history of tracking Chinese citizens both in the country and abroad in the United States, the data poses unique dangers for Chinese 23andMe customers who may become targets of the Chinese government's surveillance and intimidation apparatus.

7. To this day, 23andMe has never told its 7 million compromised customers that their PGI was disclosed on the dark web, and never told its Jewish and Chinese customers that they were specifically targeted. These customers must be immediately notified of the true nature of the breach so that they can protect themselves and take the steps necessary to remove their PGI off Defendant's platform if they so choose.

8. As explained below, 23andMe lied to customers about how it would protect their data, failed to reasonably protect their data in accordance with industry standards, lied about the scope and severity of the breach, failed to notify its Jewish and Chinese customers that they were specifically targeted, and in the end, exposed them to a host of threats and dangers that they'll never see coming. These customers would not have purchased genetic testing kits or provided their genetic information to 23andMe had they known that it would fail to protect their data or conceal information critical to their safety and well-being.[1]

9. Accordingly, Plaintiffs bring this class action on behalf of themselves, a Vulnerable Persons Subclass, and a State Genetic Privacy Statute Subclass to hold 23andMe accountable for its egregious misconduct and to force it to notify its customers, including specifically its Jewish and Chinese customers, of the actual scope and extent of the breach.

PARTIES

10. Plaintiff David Melvin is a natural person and a citizen of the State of Illinois.

11. Plaintiff J.L. is a natural person and a citizen of the State of Florida.

12. Defendant 23andMe, Inc., is a Delaware corporation with its principal place of business located at 349 Oyster Point Boulevard, San Francisco, California 94080.

[1] There may be additional ethnic, racial, or otherwise vulnerable groups that were specifically targeted by the breach, which is an issue that counsel will explore through discovery.

JURISDICTION AND VENUE

13. This Court has original jurisdiction over this action under 28 U.S.C. § 1332(d)(2). The amount in controversy exceeds the sum or value of $5 million, exclusive of interests and costs, there are more than 100 members of the proposed Classes, and at least one Class Member is a citizen of a state different from Defendant.

14. This Court has personal jurisdiction over Defendant because Defendant is headquartered in California, its principal place of business is in California, and it regularly conducts business in California.

15. Venue is proper in this District under 28 U.S.C. § 1391(b) because Defendant and/or its parents or affiliates are headquartered in this District and a substantial part of the events or omissions giving rise to Plaintiffs' claims occurred in this District.

DIVISIONAL ASSIGNMENT

16. Pursuant to Civil Local Rule 3-2(c)&(d), this case should be assigned to the San Francisco Division because a substantial part of the events or omission giving rise to the claim occurred within the county of San Mateo.

STATEMENT OF FACTS

I. 23andMe Creates and Stores the Highly Sensitive Genetic Profile Reports of its Customers.

17. 23andMe is a leading biotechnology company founded with the mission "to help people access, understand, and benefit from the human genome." It offers a suite of services including DNA analysis, genetic healthcare information, and genetic ancestry analysis services and touts its ability to provide users with "direct access to genetic information."

18. In order to use Defendant's services, customers buy one of the various packages that 23andMe offers, which currently range in prices from $119 to $298. Defendant analyzes the DNA in the customer's saliva sample and provides a detailed personalized report of their genetic profile.

19. 23andMe creates reports for its customers that provide extraordinarily detailed information derived from their individual genome—in other words, an intimate snapshot of

their genetic profile. The report includes the individual's health risks and disease profile, which can include predisposition and carrier status for certain cancers, Alzheimer's disease, diabetes, cystic fibrosis, sickle cell anemia, and other conditions. In addition to this information, reports also include information about the individual's ethnic and ancestral background, genetic health risks, as well as pharmacogenetic information—how their body processes certain medications.

20. Beyond personalized reports, 23andMe also offers a "DNA Relatives" feature that allows customers to share data with other customers and "explore the genetic similarities and differences between you and family members." Information shared through this feature includes, but is not limited to, the name of individual account holders, percentage of shared DNA and predicted relationships, ancestry reports, geographic location, family names, profile pictures, birth years, family trees, and more.

II. 23andMe Promised its Customers that it Would Protect Their Private Genetic Information Using Security Measures that "Exceed" Industry Standards.

21. To convince customers to pay money for its testing services, 23andMe promises them that privacy and security are paramount to its business operations.

22. 23andMe recognizes the sensitive nature of genetic information and assures customers that "your privacy comes first" and that "when you explore your DNA with 23andMe, you entrust us with important personal information. That's why, since day one, protecting your privacy has been our number one priority. We're committed to providing you with a safe place where you can learn about your DNA knowing your privacy is protected."

23. 23andMe also tells customers that it is "a safe place to explore and understand your genes," because "Privacy and Security are woven into everything we do" and "respect for customer privacy and transparency are core principles" that help "maintain customer trust."

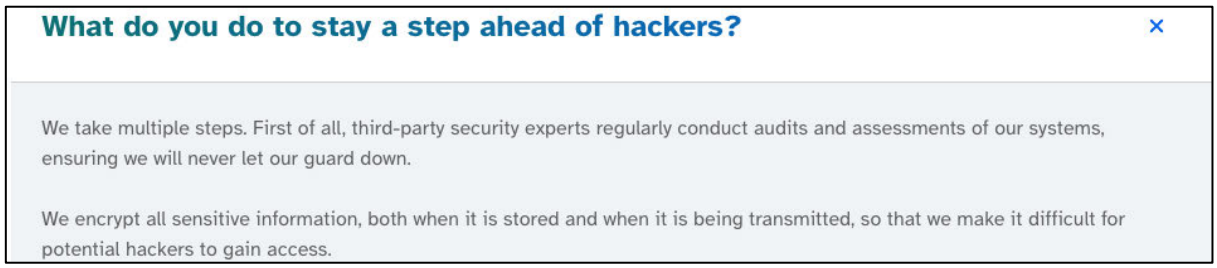
24. In its privacy policy, 23andMe acknowledges that it has obligations to protect the data customers provide, stating, "we appreciate the level of trust [customers] put into us" and telling customers it has implemented "physical, technical, and administrative measures aimed at preventing unauthorized access to or disclosure of your Personal Information."

25. In addition to recognizing the importance of privacy to its customers, 23andMe

represents that genetic information is "fiercely protected by security practices that are regularly reviewed and updated." It further states that "your genetic information deserves the highest level of security, because without security, you can't have privacy" and reiterates that it "employs software, hardware, and physical security measures to protect [user] data."

26. 23andMe further assures customers that its data security protocols "exceed industry data protection standards," that it "encrypt[s] all sensitive information," and also "conduct[s] regular assessments to identify security vulnerabilities and threats."

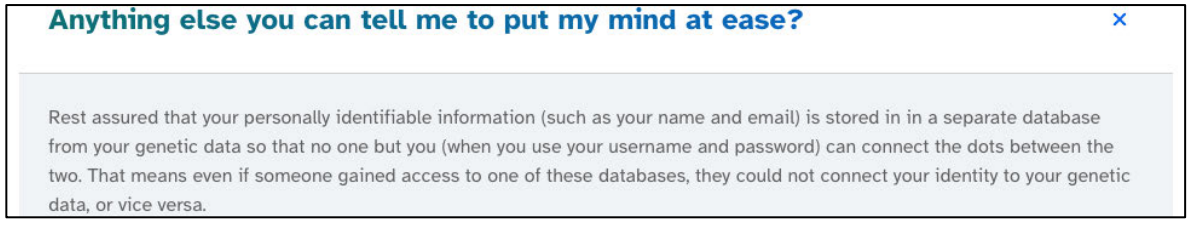
27. 23andMe also expressly tells users that it understands the threat of hackers and the severity of the consequences of a potential data breach, as shown in Figure 1 below, which is a screenshot from its website.



(**Figure 1.**)

28. On its blog, the company goes further, stating that "23andMe access combines token-based, multi-factor authentication and strict least-privileged authorization controls."

29. Defendant also tells potential customers that they should not be concerned about their private genetic information being exposed because the company untethers its customers' identities from the genetic data stored on its servers. In response to a hypothetical question, "Anything else you can tell me to put my mind at ease," Defendant promises that personally identifiable information is segregated from genetic data, so that "no one but you . . . can connect the dots between the two," as shown in Figure 2 below, which is a screenshot from its website.



(Figure 2.)

30. In other words, 23andMe assures customers that even if breached, their PGI will remain protected and unconnected to their identities.

31. These statements are meant to assure customers that their PGI will not be at risk of disclosure and that they have full control over how it is shared. This message is bolstered by representations from 23andMe that "you are in control of your DNA and your data" and "we give you full control to decide how your information is used and with whom it is shared."

32. 23andMe's customers chose to purchase the company's services with the expectation that it would comply with its promises to keep such information confidential and secure from third parties.

33. While 23andMe assured customers of the numerous steps it takes to protect their privacy, the data breach announced on October 6, 2023 has shown these representations to be false, including the specific promises to anonymize PGI stored on its servers, protect PGI using protocols that "exceed" industry standards, and actively monitor for suspicious activity.

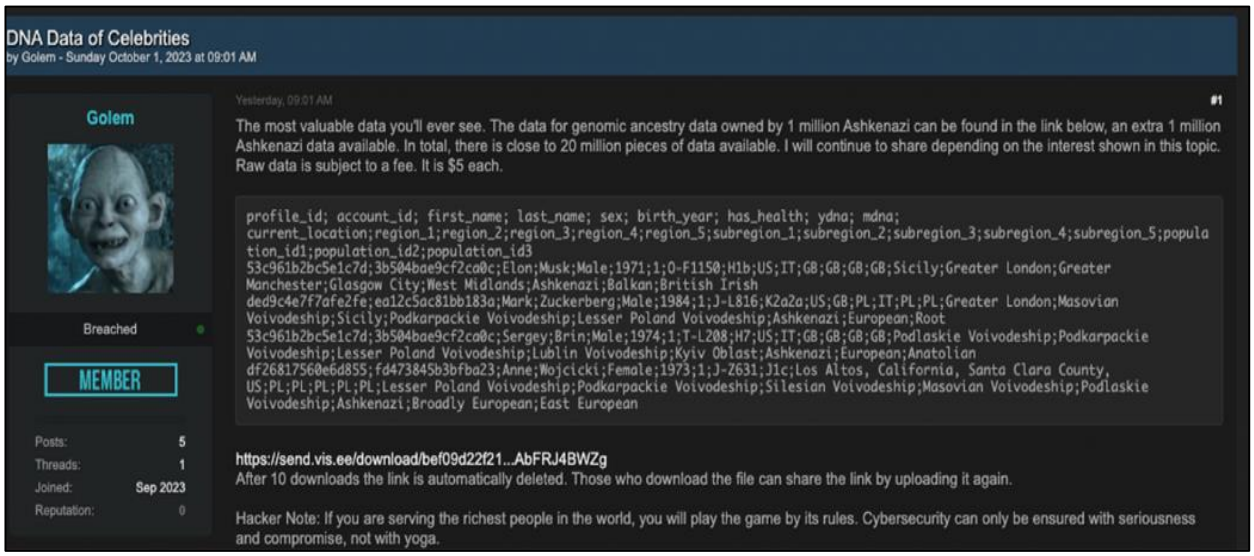
III. Despite its Data Security Promises, 23andMe's Customers' Private Genetic Information was Stolen and Used to Target Vulnerable Groups.

34. Hackers use the "dark web" to buy, sell, and otherwise release stolen data. The dark web is accessible via TOR (The Onion Router), which redirects traffic through thousands of relays in order to anonymize the user's internet activity and browsing. While using TOR, the websites that are visited only log the IP address of the last TOR relay, as opposed to the user's actual IP address. TOR mainly consists of Onion sites that are similar to normal websites but end with an address of ".onion." These sites can only be visited through a TOR interface. Just like the surface web, the dark web has various search engines that can be used to find content.

35. Cybercrime forums such as Breach Forums are utilized by users on the dark web to anonymously advertise and purchase stolen information, including stolen databases, leaks from ransomware or other malicious software, and compromised accounts and passwords.

36. On October 1, 2023, a hacker using the alias "Golem" leaked the 23andMe DNA and profile data of 1 million Ashkenazi Jews, including their full names, home addresses, and birth dates on Breach Forums, calling it "[t]he most valuable data you'll ever see," as shown in

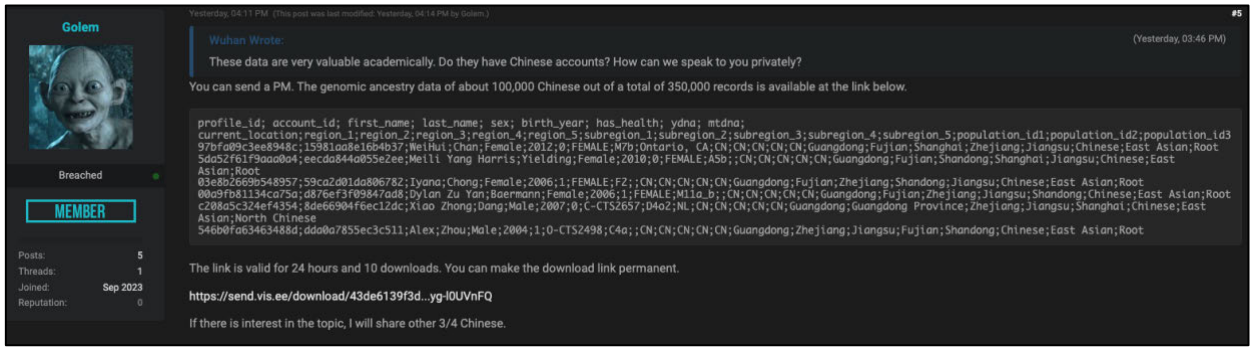
Figure 3 below, which is a screenshot from Breach Forums.



(Figure 3.)

37. Golem's explicit targeting of Jewish 23andMe users is further conveyed by his use of the character "Gollum" from The Lord of the Rings—a creature driven by greed with ugly and outsized facial features—as his profile picture.

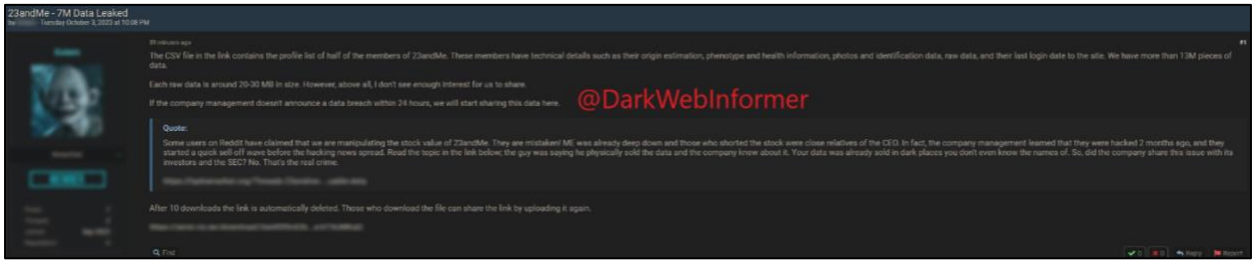
38. A few hours after leaking the Jewish 23andMe database, a user with the alias "Wuhan" replied and asked Golem if has "Chinese accounts," indicated that such data is "very valuable academically," and asked if they could "speak privately." Golem responded with a link to the DNA and profile data of 100,000 Chinese customers. Golem also stated that he has a total of 350,000 DNA and profile records and that he would release them if there was interest, as shown in Figure 4 below, which is a screenshot from Breach Forums.



(Figure 4.)

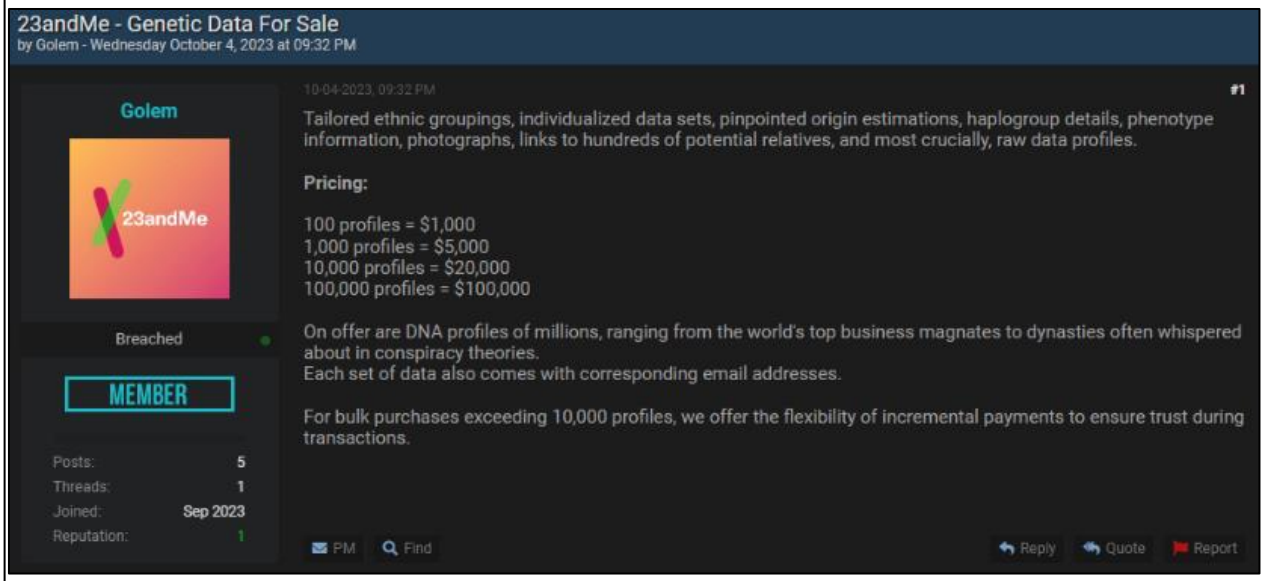
39. The next day, Golem leaked an even larger database of information including the DNA and profile data of 7 million users. Golem shared a link to the stolen data, writing, "the

CSV file in the link contains the profile list of half of the members of 23andMe . . . these members have technical details such as their origin estimation, phenotype and health information, photos and identification data, raw data, and their last login date to the site," as shown in Figure 5 below, which is a screenshot from Breach Forums taken by Dark Web Informer:



(Figure 5.)

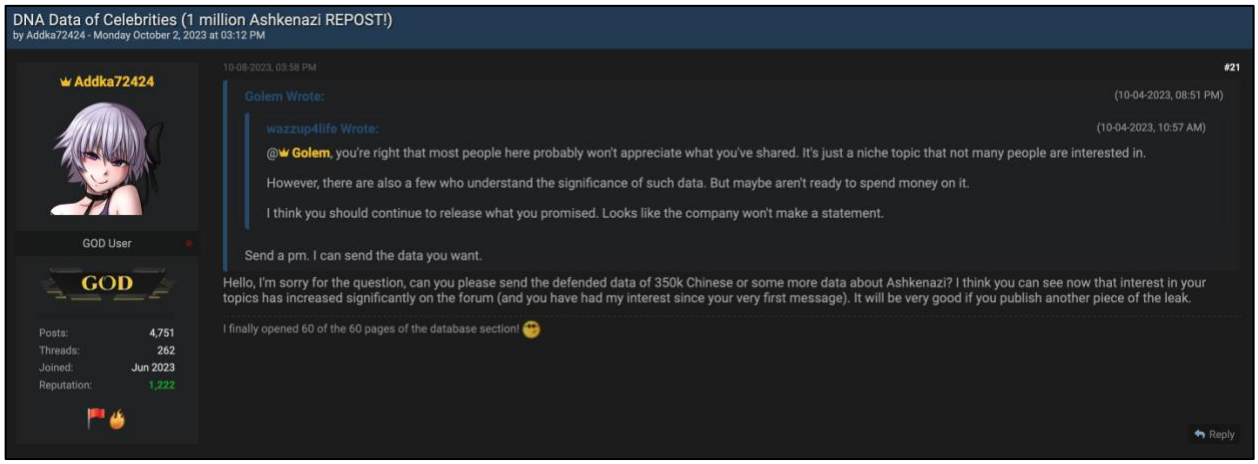
40. On October 3, 2023, Golem posted pricing for "[t]ailored ethnic groupings, individualized data sets, pinpointed origin estimations, haplogroup details, phenotype information, photographs, links to hundreds of potential relatives, and most crucially, raw data profiles," as shown in Figure 6 below, which is a screenshot from Breach Forums.



(Figure 6.)

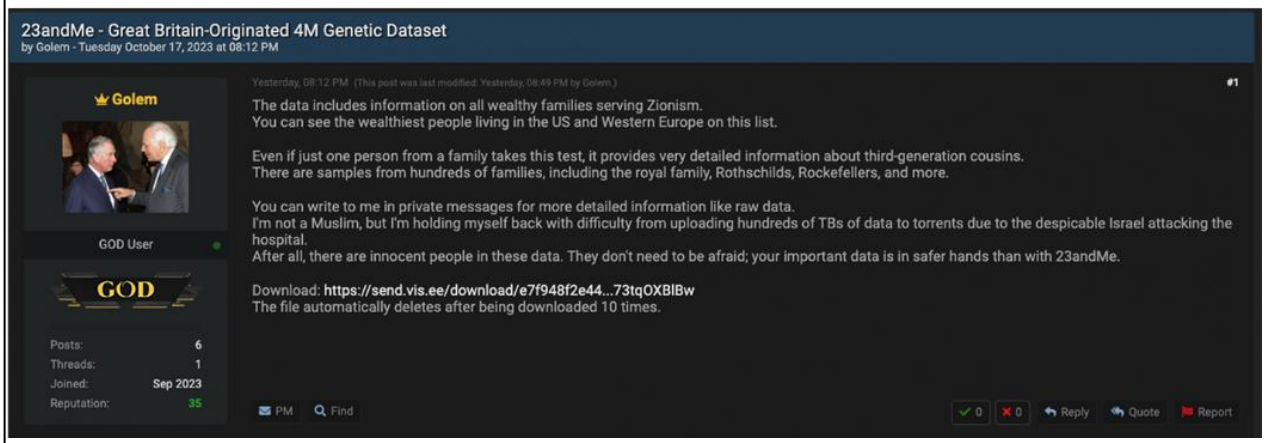
41. The Jewish and Chinese leaks were met with immediate and overwhelming interest from other Breach Forum users. For example, on October 8, 2023, "Addka72424" replied to Golem, stating, "I think you can see now that interest in your topics has increased significantly on the forum (and you have had my interest since your very first message)" and

asking, "can you please send the defended data of 350k Chinese or some more data about Ashkenazi?" as shown in Figure 7 below, which is a screenshot from Breach Forums.



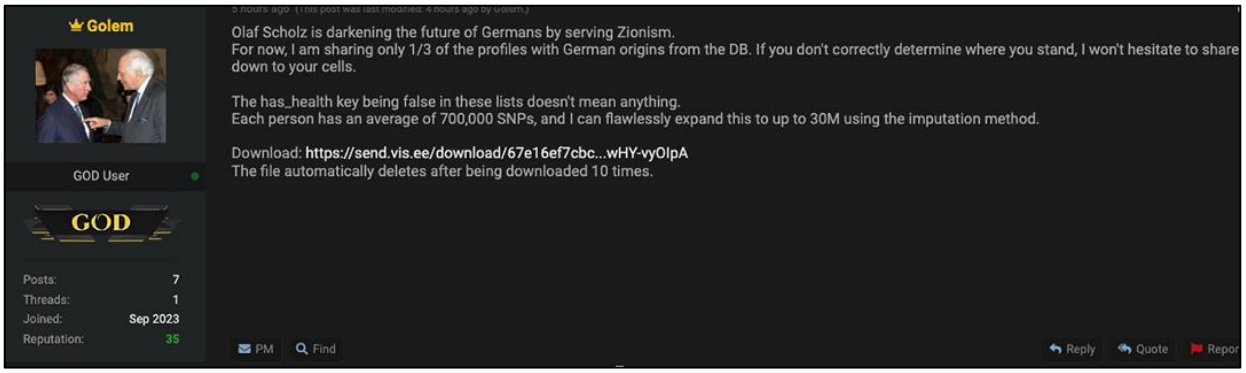
(Figure 7.)

42. On October 17, Golem posted another thread titled "23andMe – Great Britain-Originated 4M Genetic Dataset," that expounded on his apparent antisemitic agenda and included data about "wealthy families serving Zionism" and stated, "I'm not a Muslim, but I'm holding myself back with difficulty from uploading hundreds of TBs of data to torrents due to the despicable Israel attacking the hospital," shown below in Figure 8, which is a screenshot from Breach Forums.



(Figure 8.)

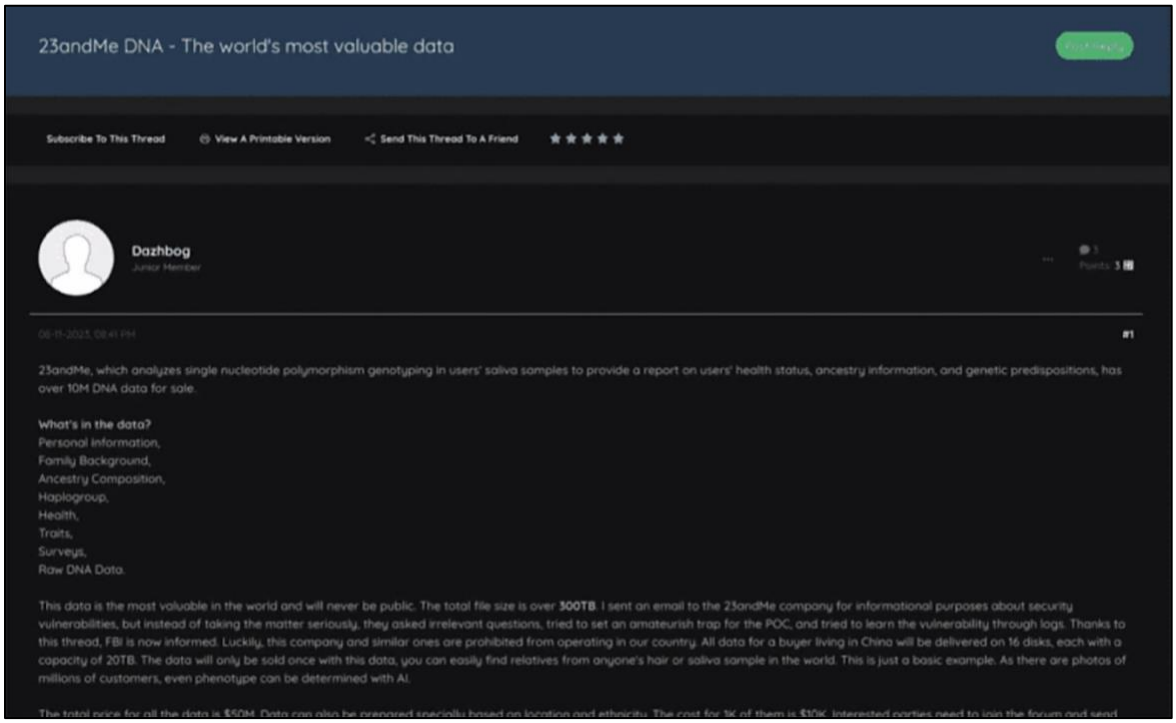
44. One day later—after German Chancellor Olaf Scholz expressed solidarity with Israel at a press conference in Tel Aviv with Israeli Prime Minister Benjamin Netanyahu—Golem posted another message stating that "Olaf Scholz is darkening the future of Germans by serving Zionism," as shown in Figure 9 below, which is a screenshot from Breach Forums.



(Figure 9.)

45. Reports show that there may have also been an additional and entirely separate breach of 23andMe's servers by a different threat actor several months before the genetic information was posted to Breach Forums on October 1, 2023.

46. On August 11, 2023, a person using the alias "Dazhbog" posted a message titled, "23andMe DNA – the world's most valuable data," on a hacker forum called Hydra Market offering to sell 300 TB of 23andMe data for $50 million and stating that "all data for a buyer living in China will be delivered on 16 disks, each with a capacity of 20 TB," as shown in Figure 10 below, which is a screenshot from Hydra Market:



(Figure 10.)

47. On August 12, 2023, Dazhbog uploaded a sample of genetic data for one million

23andMe customers in the United States, noting the leak contained the DNA profiles of 10 million Americans. The hacker claimed to have contacted 23andMe at that time—a relatively common extortion practice—but "instead of taking the matter seriously, [the company] asked irrelevant questions."

48. At this time, Plaintiffs do not know if the Dazhbog leak contained authentic 23andMe customer information or if 23andMe was even aware of the posting, as it never publicly acknowledged the post or notified its customers about it. Plaintiffs are also unaware at this time as to whether the Dazhbog and Golem leaks are related in any way. These matters will be explored through discovery.

49. But the fact that there is evidence of a potential additional breach of 23andMe's customers' genetic information that occurred two months earlier is nonetheless extremely concerning, especially given that Dazhbog provided specific instructions about how he would safely deliver this data to China and that it was offered at a price point ($50 million) that would only be relevant actors on the global stage, such as the Chinese government. People that might be considered "dissidents" to the Chinese government abroad were rightly terrified of this revelation, given the government's practice of keeping minute tabs on individuals even in other countries.

50. The disclosure of the Jewish and Chinese customer lists threatens the safety and security of those customers and subjects them to harassment, vandalism, assault, intimidation, and discrimination.

51. According to the Anti-Defamation League ("ADL"), antisemitic incidents skyrocketed after Hamas carried out a terror attack in Israel on October 7, 2023. Between October 7 and December 7, the ADL recorded a total of 2,031 antisemitic incidents, up from 465 incidents during the same period in 2022, representing a 337% increase year-over-year.[2] This includes 40 incidents of physical assault, 337 incidents of vandalism, and 749 incidents of

[2] Press Release, ADL, *ADL Reports Unprecedented Rise in Antisemitic Incidents Post-Oct. 7* (Dec. 11, 2023) https://www.adl.org/resources/press-release/adl-reports-unprecedented-rise-antisemitic-incidents-post-oct-7.

verbal or written harassment, and a fatality that occurred at an anti-Israel protest in Los Angeles, where a Jewish man was killed after being hit in the head by a pro-Palestinian protester.

52. A recent ResumeBuilder survey found that 25% of hiring managers are less likely to move forward with Jewish candidates, 32% reported that antisemitism is common in their workplace, and 23% admitted their belief that their industry should have fewer Jewish employees.[3]

53. In a January 11, 2024 letter to the FBI, U.S. Congressman Josh Gottheimer—a member of the House Permanent Select Committee on Intelligence—raised the alarm about the possibility that the lists could be used for domestic terrorism and expressed an urgent need "to protect the information, locations, and lives of the American Jewish population":

> I am concerned that the leaked data could empower Hamas, their supporters, and various international extremist groups to target the American Jewish population and their families. The threat of violent domestic extremism poses a significant danger to America's Jewish community.

54. Likewise, Arizona Attorney General Kris Mayes recently sent a letter to 23andMe expressing her concerns for the safety of its Jewish and Chinese customers:

> The recent increase in all hate crimes across the country, especially antisemitic and anti-Asian hate crimes, means that this is a particularly dangerous time for the targeted sale of information of individuals identifying and belonging to specific racial or ethnic groups—information that 23andMe profits from analyzing.

55. Given the Chinese government's long history of tracking Chinese citizens both in the country and abroad in the United States, the data breach poses unique dangers for 23andMe customers of Chinese ancestry who may become targets of the Chinese government's surveillance and intimidation apparatus.

56. In fact, a secret Chinese police station was recently discovered in New York City that was tasked with monitoring and coercing Chinese expatriates.[4] The station was part of an

---

[3] *1 in 4 hiring managers say they are less likely to move forward with Jewish applicants*, ResumeBuilder, https://www.resumebuilder.com/1-in-4-hiring-managers-say-they-are-less-likely-to-move-forward-with-jewish-applicants/ (last updated Jan. 9, 2024).

[4] Perry Stein and Joseph Menn, *U.S. alleges secret Chinese police post in NYC, online tracking of dissidents*, The Washington Post (Apr. 17, 2023), https://www.washingtonpost.com/national-security/2023/04/17/chinese-police-new-york-social-media/.

extensive network that the Chinese government uses to silence dissent and exert control of Chinese nationals and dissidents in the United States.

57. This breach also raises the specter of Chinese nationals being coerced within the vast ambit of China's social credit system, which can severely limit personal freedoms based on behavior. The system can dictate one's access to services, freedom of movement, and even influence social standing. The pervasive nature of this system means that the compromised data from 23andMe could place individuals and their families under even greater scrutiny, potentially leading to punitive measures that extend beyond China's borders.

58. To this day, Defendant has failed to notify any of its Ashkenazi Jewish or Chinese customers that their DNA, genetic reports, and personal information has been leaked on Breach Forums and shared with an untold number of hackers.

59. For customers of Ashkenazi Jewish and Chinese ancestry, the stakes could not be higher. The uncertainty surrounding which other ethnic or religious groups may be targeted with the leaked PGI database only adds to the distress. In a climate where cyber threats loom large, the possibility that hackers could aggregate and trade sensitive genetic information about vulnerable communities represents a harrowing breach of trust and personal security.

IV. Instead of Taking Responsibility for its Deficient Data Security Measures, 23andMe Drastically Downplayed the Breach and Blamed its Customers.

60. Though its customers' PGI was posted on Breach Forums on October 1, 2023, 23andMe waited 5 days before announcing through a vaguely drafted blog post that it "recently learned that certain 23andMe customer profile information . . . was compiled from individual 23andMe.com accounts without the account users' authorization" as a result of "threat actors" being able to "access certain accounts" (the "October 6 Announcement").

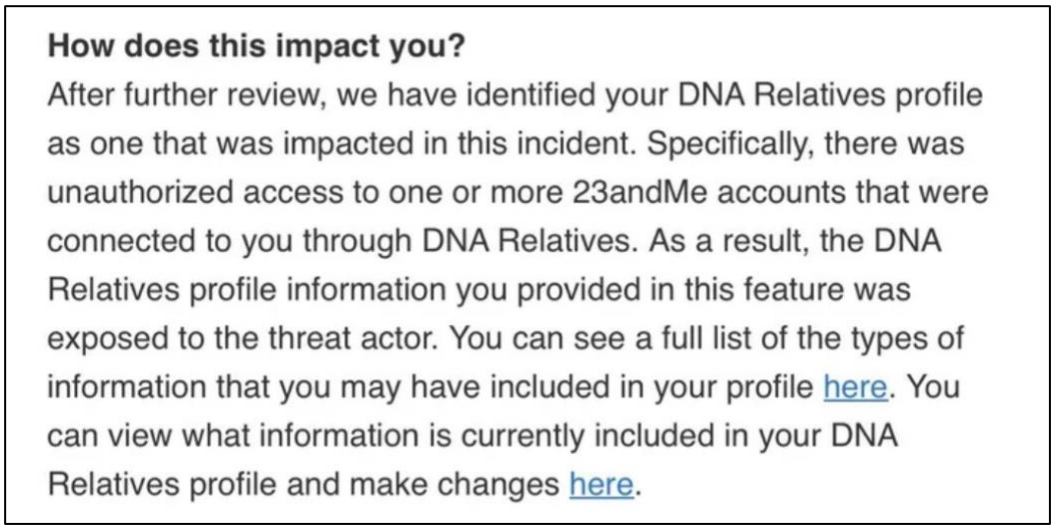
61. The October 6 Announcement failed to provide any details on the number of customers affected by the breach, and most importantly, failed to mention that the hacker leaked the DNA and profile information of 7 million customers on the dark web or that the hacker disclosed specially curated lists of Jewish and Chinese customers. In fact, to this day, 23andMe has never told its customers about the Breach Forums leak, even though its

spokesperson has confirmed for multiple media outlets that the leak contained genuine data.

62. Instead of providing this critical information or explaining what steps were being taken to remedy its data security vulnerabilities, 23andMe's October 6 Announcement shifted the blame to its customers, telling them that the breach was the result of "threat actors [who] were able to access certain accounts in instances where users recycled login credentials—that is, usernames and passwords that were used on 23andMe.com were the same as those used on other websites that have been previously hacked." 23andMe also reassured that customer data is adequately protected on its system, reiterating that "At 23andMe, we take security seriously. We exceed industry data protection standards and have achieved three different ISO certifications to demonstrate the strength of our security program. We actively and routinely monitor and audit our systems to ensure that your data is protected."

63. Over the next two months, 23andMe released a handful of minor updates that failed to provide any meaningful or substantive information about the breach. For example, 23andMe updated its October 6 Announcement on October 20, 2023 to say that "As part of the ongoing security investigation, we have temporarily disabled some features within the DNA Relatives tool as an additional precaution to protect the privacy of our customers," and again on November 6, 2023 to say that "[s]tarting today, we are requiring all customers to utilize email 2-step verification (2SV) as an added layer of protection for their account." The updates were silent about the scope and extend of the breach, despite that it already had actual knowledge that the DNA and profile information of 7 million customers was leaked on Breach Forums.

64. Two months later, on December 1, 2023, Defendant updated its October 6 Announcement to report that "23andMe has completed its investigation, assisted by third-party forensic experts," and is finally "in the process of notifying affected customers." In other words, 23andMe waited a full two months before it informed 7 million customers that they were directly impacted by the data breach, and even then, the section titled '"How does this impact you?" was so vague and confusing that it raised more questions than it answered, as shown in Figure 11 below, which is a screenshot of that section from 23andMe's December 1, 2023 email notice:



How does this impact you?

After further review, we have identified your DNA Relatives profile as one that was impacted in this incident. Specifically, there was unauthorized access to one or more 23andMe accounts that were connected to you through DNA Relatives. As a result, the DNA Relatives profile information you provided in this feature was exposed to the threat actor. You can see a full list of the types of information that you may have included in your profile here. You can view what information is currently included in your DNA Relatives profile and make changes here.

(Figure 11.)

65. Amazingly, Defendant again concealed the Breach Forums leak and again failed to notify customers with Ashkenazi Jewish or Chinese ancestry that they were specifically targeted by hackers.

66. On December 5, 2023, Defendant provided a final blog update to its October 6 Announcement:

> As our investigation comes to a close, we wanted to share the details of what took place and our findings.
>
> In early October, we learned that a threat actor accessed a select number of individual 23andMe.com accounts through a process called credential stuffing. That is, usernames and passwords that were used on 23andMe.com were the same as those used on other websites that have been previously compromised or otherwise available. We do not have any indication that there was a data security incident within our systems, or that 23andMe was the source of the account credentials used in these attacks.
>
> The threat actor used the compromised accounts to access information shared with these accounts. Specifically, DNA Relatives profiles connected to these compromised accounts, which consist of information that a customer chooses to make available to their genetic relatives when they opt in to participate in 23andMe's DNA Relatives feature. A DNA Relatives profile includes information such as display name, predicted relationships, and percentage of DNA shared with matches. You can find a full list of the types of information included in a DNA Relatives profile here.
>
> Additionally, through the compromised accounts, the threat actor accessed a feature called Family Tree, which includes a limited subset of DNA Relatives profile information. The Family Tree feature does not include ancestry information such as the percentage of DNA shared with genetic matches or ancestry reports.

Additional Details

- The threat actor was able to access less than 0.1%, or roughly 14,000 user accounts, of the existing 14 million 23andMe customers through credential stuffing.
- The threat actor used the compromised credential stuffed accounts to access the information included in a significant number of DNA Relatives profiles (approximately 5.5 million) and Family Tree feature profiles (approximately 1.4 million), each of which were connected to the compromised accounts.

Since detecting the incident, we emailed all customers to notify them of the investigation and are continuing to notify impacted customers, based on applicable laws. We also required every 23andMe customer to reset their password. In addition, 23andMe now requires all new and existing customers to login using two-step verification. Protecting our customers' data privacy and security remains a top priority for 23andMe, and we will continue to invest in protecting our systems and data.

67. 23andMe's final public announcement fell woefully short of providing any information about the breach and again failed to warn victims that their private information had already been leaked on Breach Forums. By failing to disclose this critical information, 23andMe lied to its customers about the scope and severity of the breach.

68. Further, despite having actual knowledge that the hacker curated and leaked lists of Jewish and Chinese customers on the dark web, a 23andMe spokesperson told the New York Times on December 4, 2023 that "we have not learned of any reports of inappropriate use of the data after the leak."[5] Likewise, 23andMe's attorney, Ian Ballon, went even further in a December 11, 2023 letter to attorneys representing certain 23andMe customers, stating, "the information that was potentially accessed cannot be used for any harm."[6] These were false statements that were intended to mislead 23andMe's customers and investors.

V. Despite Blaming its Customers, the Circumstances of the Breach Show that 23andMe Failed to Implement Basic Security and Threat Detection Measures.

69. The facts underlying the breach, as well as the October 6 Announcement and all

[5] Rebecca Carballo, *Data Breach at 23andMe Affects 6.9 Million Profiles, Company Says*, New York Times (Dec. 4, 2023), https://www.nytimes.com/2023/12/04/us/23andme-hack-data.html.

[6] Letter from Ian C. Ballon, Attorney for 23andMe, to Hassan A. Zavareei (Dec. 11, 2023) available at https://www.documentcloud.org/documents/24252535-response-letter-to-tycko-zavareei-llp.

updates thereafter, demonstrate that 23andMe abjectly failed to implement reasonable and adequate security measures prior to the October 6 Announcement by (1) failing to implement reasonable policies and procedures to detect suspicious activity; (2) failing to adequately anticipate and prevent reasonably foreseeable hacking threats; (3) failing to properly assess the security and privacy risk of dangerous product features (such as DNA Relatives); and (4) failing to respond to public discussions of leaks of data in Defendant's possession.

70. First, 23andMe very obviously failed to take the proper steps to detect and prevent the unauthorized access. Credential stuffing generally has a very low rate of success at around 0.1%—meaning a threat actor will succeed only once for every thousand attempts to use a recycled password from a large list.[7] The fact that 23andMe admits roughly 14,000 accounts were successfully accessed means the threat actor likely made around *14 million failed login attempts*. If 23andMe had even basic threat detection tools in place, it would have detected such a large pattern of suspicious activity in real time and had ample opportunity to shut it down. Similarly, the automated process by a threat actor to access 5-7 million DNA Relatives profiles also presents a very obvious anomalous pattern of access that would appear very different from normal user activity to threat detection protocols.

71. Had 23andMe implemented adequate monitoring systems in line with industry guidance, it could have detected these patterns of activity at the onset of the compromise and taken steps to prevent further malicious logins as well the further access to and eventual exfiltration of its customers' highly sensitive genetic data.

72. 23andMe also failed to adequately anticipate and prevent reasonably foreseeable hacking threats. Credential-stuffing attacks are a common security threat that have garnered a significant amount of attention due to breaches at other large companies by hackers using recycled user passwords. For this type of attack, hackers often buy credentials from these previous breaches, knowing that users often reuse passwords. 23andMe was well aware of the

[7] CloudFlare, *What is Credential Stuffing?* https://www.cloudflare.com/learning/bots/what-is-credential-stuffing/#:~:text=Statistically%20speaking%2C%20credential%20stuffing%20attacks,they%20will%20succeed%20roughly%20once (last visited Jan. 23, 2024).

threat of this type of attack and even posted warnings in its privacy policies writing, "[b]e mindful of keeping your password and other authentication information safe from third parties, and immediately notify 23andMe of any unauthorized use of your login credentials." Despite this knowledge, 23andMe apparently placed the burden on users of the platform to report unusual activity, when it could have proactively protected customer information by requiring them to use multi-factor authentication for their accounts—a feature that had been optional on the platform since 2019.

73. In fact, 23andMe implicitly admitted that the breach could have been prevented with two-step verification. On November 6, 2023—more than a month after the Breach Forum leak—23andMe finally began requiring customers to use two-step verification because it "provides an extra layer of security and can prevent bad actors from accessing an account through recycled passwords." Many companies have had mandatory two-step verification in place for years. Ring, a leading manufacturer of home security systems and cameras, added the requirement roughly four years ago. Had 23andMe implemented industry standard protections (or "exceed" them as promised), it would have required two-step verification prior to this breach.

74. Beyond two-step verification, the Open Source Foundation for Application Security ("OWASP"), a peer-reviewed industry resource, provides a number of basic, industry standard measures that 23andMe could have implemented to protect against a credential-stuffing attack including, implementing a Completely Automated Public Turing test to tell Computers and Humans Apart (CAPTCHA) for each login attempt, blocking known malicious or abusive IP addresses or devices, or even requiring users to create a username as opposed to an email address (which would have been listed in illicit information obtained by hackers to conduct a credential-stuffing attack).[8] Had 23andMe implemented *any* of these security processes, the credential-stuffing attack could have been thwarted entirely.

[8] *Credential Stuffing Prevention Cheat Sheet*, OWASP, https://cheatsheetseries.owasp.org/cheatsheets/Credential_Stuffing_Prevention_Cheat_Sheet.html (last visited Jan. 23, 2024).

75. Before the breach, 23andMe also failed to inform users of the increased risks of using the DNA Relatives feature. 23andMe knew or should have known through a risk assessment that the DNA Relatives function could compromise the integrity of numerous customer profiles if a single associated account was breached. Nevertheless, there were no additional safeguards, protections, or warnings in place to alert users to increased threats when using this feature. If users had known of the potential for the widespread compromise of user accounts through this feature, they would have likely opted out.

76. The unauthorized acquisition of such a massive amount of user data during the breach further showed that 23andMe failed to institute reasonable security measures to prevent or detect the attack including, monitoring for unusual login patterns and rates, utilizing up-to-date audit and traceability tools to monitor for suspicious activity, as well as threat detection and monitoring alerts that trigger when in real time data is exfiltrated at large volumes. Any of these basic security measures would have detected and mitigated the credential-stuffing attack and unauthorized data scraping of the DNA Relatives function.

77. While 23andMe publicly touted that it was certified in information security standards such as ISO/IEC 27001:2013, 27018, and 27701, it failed to upgrade its certifications to the newer 2022 versions, which contained pertinent policies that could have addressed the potential sources of the breach described here. For example, the new controls in updated versions include topics of threat intelligence, data leakage prevention, and monitoring activities, all of which are relevant to this breach.[9]

78. 23andMe also knew or should have known about industry best practices aimed at preventing common data security threats, including a credential-stuffing attack. OWASP Top 10, a peer-reviewed industry standard document, highlighted the top web vulnerabilities against which companies should defend themselves.[10] Among these threats, the category "Identification and Authentication Failures" highlights security weakness that "permit

[9] *ISO/IEC 27001& ISO/IEC 27002:2022: What You Need to Know*, PECB (Mar. 23, 2022) https://pecb.com/past-webinars/isoiec-27001--isoiec-270022022-what-you-need-to-know.
[10] *OWASP Top 10: 2021*, OWASP, https://owasp.org/Top10/ (last visited Jan. 23, 2024).

automated attacks such as credential stuffing."[11] Another category, "Security Logging and Monitoring Features" outlines best practices to "detect, escalate, and respond to active breaches" including appropriate alerting thresholds, monitoring logins and high-value transactions, and monitoring suspicious activities.[12]

79. 23andMe also failed to comply with guidance promulgated by the Federal Trade Commission ("FTC") to ensure businesses handling confidential consumer information implement adequate data security practices.[13] With respect to detecting data breaches, in particular, the FTC recommends businesses use an intrusion detection system, monitor all incoming traffic to the networks for unusual activity, monitor for large amounts of data being transmitted from their systems, update systems frequently, and have a response plan prepared in the event of a breach. The failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data is considered an unfair act or practice prohibited pursuant to Section 5 of the FTC Act, 15 U.S.C. § 45, and state law equivalents.

80. Finally, 23andMe failed to implement digital threat monitoring systems to obtain visibility into the surface web (the regular open internet), the deep web (sites that require logins), and the dark web (sites only accessible via special software such as TOR). The main

---

[11] *A07:2021—Identification and Authentications Failures*, OWASP, https://owasp.org/Top10/A07_2021-Identification_and_Authentication_Failures/ (last visited Jan. 23, 2024).

[12] *A09:2021 — Security Logging and Monitoring Failures*, OWASP, https://owasp.org/Top10/A09_2021-Security_Logging_and_Monitoring_Failures/ (last visited Jan. 23, 2024).

[13] The FTC has also issued guidance related to security principles and standard practices for businesses handling confidential information. These include but are not limited to: (a) taking inventory of the personal customer information they collect and store; (b) properly disposing of personal information and only keeping it for as long as necessary; (c) protecting confidential information through physical security, electronic security (including encryption and authentication), and employee training; (d) understanding their network's vulnerabilities; and (e) implementing policies to correct security problems. *See Protecting Personal Information: A Guide for Business*, FTC (Oct. 2016), https://www.ftc.gov/business-guidance/resources/protecting-personal-information-guide-business; *see also Policy Statement of the FTC on Biometric Information and Section 5 of the FTC Act*, FTC (May 18, 2023), https://www.ftc.gov/system/files/ftc_gov/pdf/p225402biometricpolicystatement.pdf (including genetic information within the definition of "biometric information" which must be protected by reasonable security measures to prevent unauthorized access).

purpose of such monitoring is to gain early warning to better anticipate and detect a breach. Many companies run their own threat intelligence programs and others either rely completely on a third party or use that third party to augment their existing program.

81. The surface web can be scanned by simply using various search engine operators to look for a particular company name or product identifying them. Google can also be used to set alerts to fire if a particular keyword is mentioned on the surface web. Searching the deep web often involves creating logins to various known cybercriminal sites and checking forums for particular mentions. Just like the surface web, the dark web has various search engines that can be used to find content. Additionally, threat intelligence sources often provide large lists of various cybercrime related Onion sites.

82. If consumers had known that 23andMe failed to comply with its own security statements, industry best practices, and reasonable security standards, they would not have purchased or chosen to entrust 23andMe with highly confidential information such as their genetic or personal information.

83. While the 23andMe had the resources necessary to prevent, or at the very least, detect and mitigate the breach, it neglected to abide by its own terms and security promises, failed to implement basic measures designed to anticipate and prevent reasonably foreseeable hacking threats, and failed to implement reasonable policies to detect suspicious activity.

VI. As a Company Storing Highly Valuable Private Genetic Information, 23andMe Knew or Should Have Known that it Would Likely be Targeted by Hackers.

84. 23andMe was not only entrusted with protecting users' personal information but also their highly sensitive genetic information. While the unauthorized disclosure of personal information can have significant consequences, the unauthorized disclosure of genetic information compounds these issues and poses unique risks that have the potential to inflict permanent and irreparable harm.

85. 23andMe knew that its data security obligations were important given the increase in cyberattacks targeting companies that store confidential consumer information. For example, the Identity Theft Resource Center estimated that as of the third quarter of 2023, there

were approximately 2,116 reported data breaches impacting over 233 million people.

86. Research has shown that personal data has high commercial value on the dark web, where information such as names, addresses, phone numbers, and credit history of individuals sells for between $40 and $200.[14] Beyond the monetization of individual-level information, reports have also documented the significant commercial value of access to the breached databases of companies.

87. Beyond its obligations regarding personal information, 23andMe knew or should have known that the unauthorized disclosure of genetic information poses an even higher risk to consumers because it is immutable, thereby making its disclosure harder, if not impossible, to cure. This immutability also makes genetic data highly attractive to third parties. Genetic data is unique in the value it represents to both a victim of a data breach and the hacker obtaining the data because, "[o]nce digital genetic data is stolen or disclosed, it cannot be reissued or changed in the same manner as other information types. A single human whole genome sequence can cost hundreds to thousands of dollars per sample, and when amassed, genetic information of large cohorts can be worth millions of dollars. This positions human genetic information systems as likely targets for cyber and physical attacks. . . ."[15]

88. The National Counterintelligence and Security Center has warned consumers about the risks posed by the disclosure of genetic information, advising, "your DNA is the most valuable thing you own. It holds the most intimate details of your past, present, and potential future—whether you are prone to addiction or high-risk for cancer."[16]

89. In addition to risks posed to individual customers, researchers have noted that

---

[14] *In the Dark*, VPN OVERVIEW, https://vpnoverview.com/privacy/anonymous-browsing/in-the-dark/ (last visited Jan. 15, 2024).

[15] Garrett Schumacher, et al., *Genetic Information Insecurity as State of the Art*, 8 FRONTIERS IN BIOENGINEERING AND BIOTECHNOLOGY 591980 (Dec. 8, 2020), https://www.ncbi.nlm.nih.gov/pmc/articles/PMC7768984/#:~:text=Once%20digital%20genetic%20data%20is,dollars1%20%2C2%20%2C3.

[16] Nat'l Counterintel. and Sec. Ctr., *China's Collection of Genomic and Other Healthcare Data from America: Risks to Privacy and U.S. Economic and National Security*, Dir. of Nat'l Intel. (Feb. 2021), https://www.dni.gov/files/NCSC/documents/SafeguardingOurFuture/NCSC_China_Genomics_Fact_Sheet_2021revision20210203.pdf.

one person's genetic information has implications for his or her family members and that the misuse of genetic information could have intergenerational effects that are far broader than any individual incident of unauthorized use.[17] In their words, "[s]ince genomic data contains information about a family; the impact of a breach of such data also affects the person's close and distant biological relatives, making it more significant as compared to attributes such as name, date of birth, and address of an individual."

90. The unauthorized use of genetic information can have devastating consequences for victims. It can be used to discriminate against, blackmail, and target victims based on characteristics such as ethnicity, race, or genetic predispositions.

VII. Facts Relating to Plaintiffs Melvin and J.L.

91. Plaintiff Melvin purchased a 23andMe DNA kit in or around 2010 for $400 and provided a sample of his genetic material to 23andMe for testing. At all relevant times, Plaintiff Melvin's PGI was stored and maintained on 23andMe's computer systems.

92. 23andMe notified Plaintiff Melvin in December 2023 that a threat actor compromised his account and accessed his PGI. Plaintiff Melvin was never told that his PGI was leaked on the dark web.

93. Plaintiff J.L. purchased a 23andMe DNA kit in or around 2021 and provided a sample of his genetic material to 23andMe for testing. Through this testing, Plaintiff J.L. learned that he has Ashkenazi Jewish ancestry. At all relevant times, Plaintiff J.L.'s PGI was stored and maintained on 23andMe's computer systems.

94. 23andMe notified Plaintiff J.L. in December 2023 that a threat actor compromised his account and accessed his PGI. Plaintiff J.L. was never told that his PGI was leaked on the dark web or that a hacker compiled and leaked lists of Ashkenazi Jewish customers on the dark web.

95. Plaintiff J.L. is now gravely concerned about the ramifications of appearing on a

[17] Saadia Arshad, et al., *Analysis of Security and Privacy Challenges for DNA-Genomics Applications and Databases*, 119 J. OF BIOMEDICAL INFORMATICS 103815 (July 2021), https://www.sciencedirect.com/science/article/pii/S1532046421001441#:~:text=Since%20genomic%20data%20contains%20information,and%20address%20of%20an%20individual.

list that is potentially being sold to terrorists on the dark web. He is also gravely concerned that he will become the target of harassment, intimidation, vandalism, assault, and discrimination.

CLASS ALLEGATIONS

96. Plaintiffs bring this action pursuant to the provisions of Rules 23(a), (b)(2), and (b)(3) of the Federal Rules of Civil Procedure on behalf of themselves and the following Classes:

> **Nationwide Class**: All individuals in the United States whose PGI was accessed by third parties, without consent, as a result of the data breach announced by 23andMe on October 6, 2023.
>
> **Vulnerable Persons Subclass**: All individuals in the Nationwide Class who are identified by their PGI as having Ashkenazi Jewish heritage or Chinese ancestry.[18]
>
> **State Genetic Privacy Statute Subclass**: All individuals in the Nationwide Class who reside in Illinois, Oregon, or Alaska.

97. Excluded from the Classes are the following individuals and/or entities: 23andMe and 23andMe's parents, subsidiaries, affiliates, officers, and directors and any entity in which Defendant has a controlling interest, all individuals who make a timely election to be excluded from this proceeding using the correct protocol for opting out, any and all federal, state or local governments, including but not limited to its departments, agencies, divisions, bureaus, boards, sections, groups, counsel, and/or subdivisions, and all judges assigned to hear any aspect of this litigation, as well as their immediate family members.

98. Plaintiffs reserve the right to amend the above class definitions or to propose other subclasses in subsequent pleadings and motions for class certification.

99. This action has been brought and may properly be maintained as a class action under Fed. R. Civ. P. 23 because there is a well-defined community of interest in the litigation and membership of the proposed Classes is readily ascertainable.

100. Numerosity: A class action is the only available method for the fair and efficient adjudication of this controversy. The members of the Class are so numerous that joinder of all members is impractical, if not impossible. Defendant has publicly announced that millions of

[18] Plaintiff J.L. reserves the right to expand this definition to include any additional ethnic, racial, or otherwise vulnerable populations that were specifically targeted through the breach.

accounts were affected by the breach. Membership in the Class will be determined by analysis of 23andMe's records and/or through the records made publicly available by the bad actor(s).

101. Commonality: Plaintiffs and Class Members share a community of interest in that there are numerous common questions and issues of fact and law which predominate over any questions and issues solely affecting individual members, including, but not limited to:

(a) Whether 23andMe had a legal duty to Plaintiffs and the Class to exercise reasonable care in collecting, storing, using and/or safeguarding their PGI;

(b) Whether 23andMe breached that duty when it failed to take adequate and reasonable measures to ensure its data systems were protected;

(c) Whether 23andMe's conduct, including its failure to act, resulted in or was the proximate cause of the breach of its systems, resulting in the disclosure of Plaintiffs and Class Members' PGI;

(d) Whether 23andMe engaged in unfair, unlawful, or deceptive practices by failing to safeguard Plaintiffs and Class Members' PGI;

(e) Whether 23andMe obtained written authorization from Plaintiffs and the Class before disclosing their PGI;

(f) Whether, with respect to the State Genetic Privacy Statute Subclass, Defendant's conduct violates the Illinois Genetic Privacy Act, Alaska Genetic Privacy Act, and Oregon Genetic Privacy Statutes;

(g) Whether Plaintiff Melvin and the State Genetic Privacy Statute Subclass are entitled to actual and/or statutory damages as a result of 23andMe's wrongful conduct; and

(h) Whether Plaintiffs and Class Members are entitled to injunctive and declaratory relief.

102. Typicality: Plaintiffs' claims are typical of the claims of the Class. Plaintiffs and all Class Members sustained damages arising out of and caused by 23andMe's common course of conduct in violation of law, as alleged herein.

103. Adequacy of Representation: Plaintiffs are adequate representatives of the Classes in that Plaintiffs have the same interest in the litigation of this case as the Class Members, are committed to the vigorous prosecution of this case, and have retained competent counsel who are experienced in conducting litigation of this nature. Plaintiffs are not subject to any individual defenses unique from those conceivably applicable to other Class Members or the Classes in their entirety. Plaintiffs anticipate no difficulties managing this litigation.

104. Predominance and Superiority: The Classes can be properly maintained because the above common questions of law and fact predominate over any questions affecting individual Class Members. A class action is also superior to other available methods for the fair and efficient adjudication of this litigation because individual litigation of each Class Member's claim is impracticable. Even if each Class Member could afford individual litigation, the court system could not. It would be unduly burdensome if thousands of individual cases proceed. Individual litigation also presents the potential for inconsistent or contradictory judgments, the prospect of a race to the courthouse, and the risk of an inequitable allocation of recovery among those with equally meritorious claims. Individual litigation would increase the expense and delay to all parties and the courts because it requires individual resolution of common legal and factual questions. By contrast, the class-action device presents far fewer management difficulties and provides the benefit of a single adjudication, economies of scale, and comprehensive supervision by a single court.

105. Declaratory and Injunctive Relief: The prosecution of separate actions by individual Class Members would create a risk of inconsistent or varying adjudications with respect to individual Class Members that would establish incompatible standards of conduct for Defendant. Such individual actions would create a risk of adjudications that would be dispositive of the interests of other Class Members and impair their own interests. Defendant has acted and/or refused to act on grounds generally applicable to the Classes, making final injunctive relief or corresponding declaratory relief appropriate.

FIRST CAUSE OF ACTION
Negligence
(On Behalf of Plaintiffs, the Nationwide Class, and Vulnerable Persons Subclass)

106. Plaintiffs incorporate the foregoing allegations as if fully set forth herein. Plaintiffs bring this claim on behalf of themselves, the Nationwide Class, and the Vulnerable Persons Subclass.

107. Defendant requires its customers, including Plaintiffs and the Class Members, to submit confidential PGI and personally identifiable information as a condition of receiving services, and, in return, 23andMe had a duty to safeguard their information.

108. Defendant had a duty to exercise reasonable care in protecting such information from being compromised or disclosed to unauthorized parties, including by:

(a) Designing, maintaining, and testing security protocols to ensure PGI in its possession was adequately secured and protected against common and foreseeable cyber threats;

(b) Using reasonable and adequate security procedures and systems that were/are compliant with industry-standard and best practices to timely act on warnings about data breaches; and

(c) Promptly notifying Plaintiffs and Class Members of any data breach, security incident, or intrusion that affected or may have affected their PGI.

109. Defendant had full knowledge of the sensitivity of the PGI it stored and the types of harm that Plaintiffs and Class Members could and would suffer if their PGI was wrongfully disclosed. Plaintiffs and Class Members were the foreseeable and probable victims of any inadequate security practices and procedures.

110. Defendant has admitted that Plaintiffs' and Class Members' PGI was wrongfully disclosed to unauthorized third persons as a result of the data breach.

111. Defendant breached its duties to Plaintiffs and Class Members by failing to provide fair, reasonable, or adequate data security practices to protect their PGI in ways including but not limited to:

(a) Failing to provide reasonable computer systems and data security

practices to safeguard the PGI of Plaintiffs and Class Members, including, but not limited to, the failure to require two-step verification, a known preventative against a credential-stuffing attack, the failure to utilize adequate tools and monitoring systems to flag suspicious transactions and data being exfiltrated in large volumes, and the failure to timely monitor and/or act upon online discussions of a data breach;

(b) Failing to detect in a timely manner that Plaintiffs' and Class Members' PGI and personally identifiable information had been compromised and allowing unmonitored and unrestricted access to unsecured PGI;

(c) Failing to timely and accurately disclose that Plaintiffs' and Class Members' PGI had been improperly acquired or accessed including significant details about the disclosure such as the number of impacted users and the importance of the threat to users' PGI; and

(d) Failing to timely institute security measures after the breach that could have mitigated harm and further disclosure, including the disabling of the DNA Relatives feature and immediately requiring two-step verification.

112. Defendant's willful failure to abide by these duties was wrongful, reckless, and grossly negligent in light of the foreseeable risks and known threats.

113. If Plaintiffs and the Class Members had known that Defendant failed to comply with its own security statements, industry best practices, and reasonable security standards, they would not have purchased or chosen to entrust the Defendant with highly confidential information such as their PGI or would have paid significantly less.

114. Further, as a proximate and foreseeable result of Defendant's conduct, Plaintiffs and Class Members have suffered damages and are at imminent, and even permanent, risk of additional harms and damages.

115. But for Defendant's failure to implement security measures to protect the PGI and personally identifiable information of Plaintiffs and Class Members and its negligent breach of duties owed to Plaintiff and Class Members, the PGI of Plaintiffs and the Class

would not have been compromised and/or subsequently misused by unauthorized third parties thereby harming Plaintiffs and Class Members.

116. As a direct and proximate result of Defendant's negligence, Plaintiffs and Class Members have suffered and will suffer injury, including:

(a) overpayment of monies, in that Plaintiffs and the Class members would have paid Defendant significantly less, or nothing at all, had they known about Defendant's failure to comply with its own security statements, industry best practices, and reasonable security standards;

(b) increased risk of identity theft, fraud, or misuse of their PGI;

(c) the loss of the opportunity to dictate how their PGI is used;

(d) the compromise, disclosure, and/or theft of their PGI;

(e) diminished value of their PGI; and

(f) the continued and permanent risk to their PGI.

117. Further, Plaintiff J.L. and the Vulnerable Persons Subclass have suffered additional harm in that they are now subjected to the increased threat of harassment, intimidation, vandalism, assault, and discrimination, including in the workplace.

118. Plaintiffs and Class Members are entitled to compensatory and consequential damages suffered as a result of the breach, as well as injunctive relief requiring Defendant to: (i) strengthen its data security systems and monitoring procedures; (ii) submit to future annual audits of those systems and monitoring procedures; and (iii) provide notice to all impacted customers of the actual scope and severity of the breach and inform them that their PGI has been leaked on the dark web, and with respect to the Vulnerable Persons Subclass members, inform them that they have been specifically targeted by the hacker.

SECOND CAUSE OF ACTION
Threat Assessment and Monitoring
(On Behalf of Plaintiff J.L. and the Vulnerable Persons Subclass)

119. Plaintiff J.L. incorporates the foregoing allegations as if fully set forth herein. Plaintiff J.L. brings this claim on behalf of himself and the Vulnerable Persons Subclass.

120. As a leading company in the genetic testing industry, 23andMe is well aware of

the immense value of genetic data and recognizes that such information is a prime target for cybercriminals. 23andMe also knows that people would not purchase its genetic testing kits or provide their genetic information unless they were assured that the company has implemented robust cybersecurity measures to protect their data against the persistent threat of hacking.

121. For that reason, as described above, 23andMe has made numerous and explicit promises to assure its customers that their genetic information would be properly safeguarded on its systems and protected using data protection measures that "exceed" industry standards. Even its October 6 Announcement about the breach was designed to reassure customers that their data was perfectly safe, reiterating that "At 23andMe, we take security seriously. We exceed industry data protection standards and have achieved three different ISO certifications to demonstrate the strength of our security program."

122. But for 23andMe's promises and assurance, Plaintiff J.L. and the Vulnerable Persons Subclass would not have purchased its genetic testing kits and would not have provided it with their genetic information.

123. As described above, the breach revealed for the first time that 23andMe did not implement basic, industry-standard data security measures, let alone security measures that "exceed" industry standards. As a result, 23andMe's Jewish and Chinese customers were specifically targeted by a hacker that posted their genetic information—along with their full names, home addresses, photographs, and birth dates—on the dark web hacker forum, Breach Forums. The data generated immediate interest by users around the world, and was downloaded and shared an untold number of times.

124. There can be no question as to whether the data was, in fact, downloaded by other Breach Forum users. As shown in Figures 3 and 4, above, Golem included a message beneath each of the Jewish and Chinese list download links that stated, "After 10 downloads the link is automatically deleted. Those who download the file can share the link by uploading it again." The links were deleted within an hour, meaning that the Jewish and Chinese lists were quickly downloaded 10 times by other Breach Forum users. The download links were then reposted on Breach Forums (and very likely elsewhere on the dark web) an untold number

of times thereafter.

125. The breach and subsequent disclosure of the Jewish and Chinese lists on the dark web have exposed Plaintiff J.L. and the Vulnerable Persons Subclass to ongoing and severe threats to their personal safety.

126. The individuals that downloaded the stolen Jewish and Chinese lists on the dark web can exploit them for a variety of nefarious and dangerous purposes, including to single out individuals or groups for hate crimes or other forms of harassment, intimidation, violence, and discrimination, both online and in real life.

127. The current geopolitical and social climate amplifies the risks to 23andMe's Jewish and Chinese customers. The recent Israel-Hamas war has heightened global tensions and anti-Semitic sentiment, and increased the vulnerability of Jewish communities to targeted violence and discrimination. Likewise, the Chinese government's sophisticated surveillance and intimidation apparatus presents a significant threat to Chinese customers on the list, who may face persecution or coercion in China and abroad. In this environment, the exposure of the Jewish and Chinese lists dramatically escalates the danger of being identified and located by those with hostile intentions. The geopolitical and social climate is only getting worse and underscores the urgent need to provide vigilant monitoring and protective measures for Plaintiff J.L. and the Vulnerable Persons Subclass.

128. Given the magnitude of these threats, the creation of a Threat Assessment and Monitoring Fund ("TAM Fund") is necessary to ensure the ongoing safety and well-being of Plaintiff J.L. and the Vulnerable Persons Subclass by providing the necessary funds to pay for technical and professional services, including:

(a) Dark Web Surveillance. Employ advanced cybersecurity services to conduct deep and dark web scans for any sharing of Vulnerable Persons Subclass members' personal and genetic information. This includes the use of specialized software to infiltrate and monitor darknet markets and forums where such information may be exchanged.

(b) Threat Intelligence and Protection Operations. Partner with personal

protection firm(s) and cybersecurity to collect, analyze, and operationalize in real-time threat intelligence related to the leaked data, enabling proactive identification of potential threats before they materialize and taking immediate action on threats of physical or other harm including by coordinating with relevant law enforcement authorities and dispatching personal protection personnel.

(c) Digital Footprint Analysis. Implement digital footprint analysis tools to track the digital shadows of the Vulnerable Persons Subclass members' personal information, alerting them to any unauthorized appearances on the internet.

(d) Security Advisory Services. Provide access to security consultants who can advise the Vulnerable Persons Subclass members on physical safeguards and operational security, protecting their digital identity, and responding to threats.

(e) Legal and Remediation Services. Fund professional services, including legal counsel, to advise on and take action against illicit use of the data, including through peace and/or restraining orders, cease and desist actions, and takedown demands.

(f) Public Records Sweeping. Utilize services that scan public records and request removal of any sensitive personal information linked to class members that should not be publicly available.

(g) Incident Response Team. Establish a rapid response team that can be deployed to assist Vulnerable Persons Subclass members in the event of an immediate threat, providing physical protection and technical and legal assistance.

129. These measures are designed to provide comprehensive protection and support to the Vulnerable Persons Subclass, monitor for and mitigate the ongoing risks they face, and restore confidence in their personal security and privacy following the breach.

130. Accordingly, Plaintiff J.L. respectfully seeks an order from the Court requiring 23andMe to establish a TAM Fund for the benefit of the Vulnerable Persons Subclass that is sufficiently funded to provide the services described above for a period of twenty (20) years from the establishment date, which is a reasonable period of time given the enduring nature of the threats described herein.

THIRD CAUSE OF ACTION
Violation of Cal. Bus. & Prof. Code § 17200, *et seq*.
(On Behalf of Plaintiffs, the Nationwide Class, and the Vulnerable Persons Subclass)

131. Plaintiffs incorporate the foregoing allegations as if fully set forth herein. Plaintiffs bring this claim on behalf of themselves, the Nationwide Class, and the Vulnerable Persons Subclass.

132. The California Unfair Competition Law, Cal. Bus. & Prof Code § 17200 *et seq*. ("UCL"), prohibits any "unlawful," "fraudulent," or "unfair" business act or practice and any false or misleading advertising, as defined by the UCL and relevant case law.

133. Defendant 23andMe, Inc. and Plaintiffs are "persons" under Cal. Bus. & Prof. Code § 17201.

134. By reason of Defendant's failure to take reasonable precautions to protect the PGI of Plaintiffs and the Class Members, the resulting data breach, and the unauthorized disclosure of Plaintiffs' and Class Members' PGI, Defendant engaged in unlawful, unfair, and fraudulent practices within the meaning of the UCL.

135. Defendant engaged in "unlawful" acts and practices with respect to its services by failing to establish proper security practices and procedures described herein; by soliciting and collecting Plaintiffs and Class Members' PGI with knowledge that the information would not be adequately protected; and by storing Plaintiffs' and Class Members' PGI in an unsecure electronic environment in violation of FTC guidance and industry norms, which require Defendant to use reasonable methods of safeguarding the PGI of Plaintiffs and Class Members.

136. Defendant's business practices as alleged herein are "unfair" because they offend established public policy and are immoral, unethical, oppressive, unscrupulous, and substantially injurious to consumers in that the PGI and personally identifiable information of

Plaintiffs and Class Members has been compromised for unauthorized parties to see, use, and otherwise exploit. These actions include, but are not limited to:

(a) Defendant failed to implement and maintain reasonable data security measures to protect the Plaintiffs' and Class Members' PGI;

(b) Defendant failed to identify foreseeable security risks, remediate identified risks, and adequately improve its data security in light of the highly sensitive nature of the data it maintained;

(c) To the extent Defendant may have identified a threat from duplicated account credentials, or external discussions of a breach, it did not implement timely and reasonable security measures; and

(d) Defendant's grievous conduct is unfair when weighed against the harm to the Plaintiffs and Class Members whose PGI have been compromised.

137. Defendant's failure to implement and maintain reasonable data security measures was contrary to state law—including specifically the California Genetic Privacy Act, Cal. Civ. Code § 56.18 *et seq*.— and public policy that seeks to protect consumers' personally identifiable information and ensure that entities entrusted with PGI adopt appropriate security measures.

138. Pursuant to Cal. Civ. Code § 56.181(d)(1), a direct-to-consumer genetic testing company, such as 23andMe, is required to "implement and maintain reasonable security procedures and practices to protect a consumer's genetic data against unauthorized access, destruction, use, modification, or disclosure."

139. Failure to comply with Cal. Civ. Code § 56.18 *et seq*. constitutes an unlawful practice under the UCL.

140. Defendant's failure to implement and maintain reasonable data security measures led to substantial consumer injuries as described herein, which are not outweighed by countervailing benefits to consumers or competition.

141. Defendant's business practices as alleged herein are "fraudulent" because:

(a) Defendant represented to consumers that the PGI they provided to

Defendant would remain private and secure, when in fact it has not been maintained in a private and secure manner and Defendant failed take proper measures to identify, investigate, and remediate a data breach;

(b) Defendant could and should have made a proper disclosure related to the DNA Relations feature directly to consumers to inform them of the potential for significant unauthorized disclosures through the feature;

(c) Defendant knew or should have known that its data security practices were deficient because, among other things, Defendant was aware of the sensitive nature of the information it held; and

(d) Defendant made express representations that its data security practices were sufficient to protect consumers' PGI including but not limited to, that they "exceed industry data protection standards," they "regularly conduct audits and assessment of [their] systems," and that "personally identifiable information . . . is stored in a separate database." These representations were false and misleading.

142. Plaintiffs and Class Members suffered injuries in the form of overpayment of monies, in that they would have paid Defendant significantly less, or nothing at all, had they known about Defendant's failure to comply with state law, its own security statements, industry best practices, and reasonable security standards.

143. Plaintiffs and Class Members also suffered (and continue to suffer) injury and lost money or property as a direct and proximate result of Defendant's above-described wrongful actions, inaction, and omissions, including, *inter alia*, the disclosure of their PGI and lack of notice of that disclosure.

144. But for Defendant's misrepresentations and omissions, Plaintiffs and Class Members would not have provided their PGI to Defendant or would have insisted that their data be more securely protected.

145. As a direct and proximate result of Defendant's unlawful practices and acts, Plaintiffs and Class Members were injured and lost money or property, including but not

limited to the price received by Defendant for the services, the loss of Plaintiffs' and Class Members' legally protected interest in the confidentiality and privacy of their PGI, nominal damages, and additional losses as described herein.

146. Defendant knew or should have known that Defendant's computer systems and data security practices were inadequate to safeguard Plaintiffs' and Class Members' PGI and that the risk of a data breach or theft was highly likely. Defendant's actions in engaging in the above-named unlawful practices and acts was negligent, knowing, and willful, and/or wanton and reckless with respect to the rights of Plaintiffs and Class Members.

147. Plaintiffs and Class Members lack an adequate remedy at law because the injuries here include an imminent risk of identity theft and fraud that can never be fully remedied through damages, as well as long term incalculable risk associated with medical fraud and release of genetic profiles.

148. Further, Plaintiff J.L. and the Vulnerable Persons Subclass have suffered additional harm in that they are now subjected to the increased threat of harassment, vandalism, assault, and discrimination, including in the workplace.

149. Plaintiffs, on behalf of themselves, the Nationwide Class, and the Vulnerable Persons Subclass, seek relief under Cal. Bus. & Prof. Code § 17200, *et seq.*, including, but not limited to, restitution to Plaintiffs and Class Members of money or property that Defendant may have acquired by means of Defendant's unlawful and unfair business practices, including the purchase price of the testing kits, disgorgement of all profits accruing to Defendant because of Defendant's unlawful and unfair business practices, declaratory relief, attorneys' fees and costs (pursuant to Cal. Code Civ. Proc. § 1021.5), and injunctive or other equitable relief.

150. Plaintiffs also seek injunctive relief requiring Defendant to: (i) strengthen its data security systems and monitoring procedures; (ii) submit to future annual audits of those systems and monitoring procedures; and (iii) provide notice to all impacted customers of the actual scope and severity of the breach and inform them that their PGI has been leaked on the dark web, and with respect to the Vulnerable Persons Subclass members, inform them that they have been specifically targeted by the hacker.

FOURTH CAUSE OF ACTION
Violation of the Illinois, Alaska, and Oregon Privacy Statutes
(On Behalf of Plaintiff Melvin and the State Genetic Privacy Statute Subclass)

151. Plaintiff Melvin incorporates the foregoing allegations as if fully set forth herein. Plaintiff Melvin brings this claim on behalf of himself and the State Genetic Privacy Statute Subclass, as the genetic privacy statutes in Illinois, Alaska, and Oregon are substantially similar in that all three (i) contain private rights of action, (ii) broadly cover genetic information and information derived from genetic information, and (iii) provide for statutory damages.

152. In enacting the Genetic Information Privacy Act ("GIPA"), the Illinois Legislature recognized that "[t]he public health will be served by facilitating voluntary and confidential nondiscriminatory use of genetic testing information." 410 ILCS 513/5(3); s*ee also* Alaska Stat. § 18.13.010, *et seq*.; Or. Rev. Stat. § 192.533.

153. GIPA mandates that no person may disclose the identity of any person upon whom a genetic test is performed or the results of a genetic test in a manner that permits identification of the subject of the test. *See* 410 ILCS 513/30(a); Alaska Stat. § 18.13.010; Or. Rev. Stat. §§ 192.537, 192.539.

154. Defendant is a corporation and, thus, a "person" under 410 ILCS 513/10; *see also* Alaska Stat. § 18.13.020; Or. Rev. Stat. § 192.531.

155. Plaintiff Melvin and the State Genetic Privacy Statute Subclass members provided their genetic information to Defendant and therefore provided Defendant with "genetic test[s]" and/or the "information derived from genetic testing" within the meaning of the GIPA. *See also* Alaska Stat. § 18.13.100; Or. Rev. Stat. § 192.531.

156. As explained above, Defendant disclosed Plaintiff Melvin's and the State Genetic Privacy Statute Subclass members' genetic testing and information derived from genetic testing by failing to enact or enforce adequate data security measures and policies, resulting in the data breach. *See* 410 ILCS 513/30; Alaska Stat. § 18.13.010; Or. Rev. Stat. § 192.537.

157. Defendant disclosed Plaintiff Melvin's and the State Genetic Privacy Statute Subclass members identifying information to unknown third parties by allowing them to access

their genetic information and genetic tests, in addition to personally identifying information.

158. GIPA plainly prohibits such disclosures because they contain, among other things, the results of Plaintiff Melvin's and the State Genetic Privacy State Subclass' genetic tests, including in a manner that permits identification of the subject of the test. *See* 410 ILCS 513/15 and 30; Alaska Stat. § 18.13.010; Or. Rev. Stat. §§ 192.537, 192.539.

159. Defendant did not obtain any authorization—including written authorization—from Plaintiff Melvin or the State Genetic Privacy Statute Subclass members before disclosing their genetic test results and information derived from genetic testing, as mandated by 410 ILCS 513/30(a)(2); Alaska Stat. § 18.13.010; Or. Rev. Stat. §§ 192.537, 192.539.

160. By disclosing the results of their genetic tests and information sufficient to identify Plaintiff Melvin and the State Genetic Privacy Statute Subclass members as described herein, Defendant violated Plaintiff Melvin's and the State Genetic Privacy Statute Subclass's statutorily protected rights to privacy in their genetic information under their respective state's genetic privacy statutes.

161. On behalf of himself and the State Genetic Privacy Statute Subclass, Plaintiff Melvin seeks: (1) injunctive and equitable relief as is necessary to protect the interests of himself and the State Genetic Privacy Statute Subclass members by requiring Defendant comply with the state genetic privacy statutes at issue; (2) liquidated damages or actual damages, whichever is greater, as provided by the state genetic privacy statutes at issue; and (3) costs and reasonable attorneys' fees pursuant to the state genetic privacy statutes at issue. 410 ILCS 513/40(a)(3); Alaska Stat. § 18.13.020; Or. Rev. Stat. § 192.541.

FIFTH CAUSE OF ACTION
Declaratory Judgment
(On Behalf of Plaintiffs and the Nationwide Class)

162. Plaintiffs incorporate the foregoing allegations as if fully set forth herein. Plaintiffs brings this claim on behalf of themselves and the Nationwide Class.

163. Under the Declaratory Judgment Act, "any court of the United States, upon the filing of an appropriate pleading, may declare the rights and other legal relations of any interested party seeking such declaration, whether or not further relief is or could be sought."

28 U.S.C. § 2201(a). This count is brought under the federal Declaratory Judgment Act, 28 U.S.C. §§ 2201, *et seq*., which authorizes the Court to enter a judgment declaring the rights and legal relations of the parties and grant further necessary relief. The Court has broad authority to restrain acts, such as here, that are tortious and violate the state statutes described herein.

164. An actual controversy has arisen in the wake of the data breach.[19] Defendant has attempted to block Plaintiffs' access to justice and redress through surprise and unfair arbitration provisions that it added to its Terms of Service ("TOS") on November 30, 2023. Defendant delayed sending notice to impacted customers for two months so that it could first update its TOS to insulate itself from the fallout.

165. Defendant continues to possess the genetic information of Plaintiffs and Class Members who remain subject to the TOS.

166. Defendant's material changes to the arbitration provisions in its TOS are designed to intentionally constrain Plaintiffs' and the Class's legal rights. Defendant inserted new language, TOS § 5(a) which prohibits Plaintiffs from initiating any arbitration or court proceeding for at least sixty days after delivery of a "valid" notice of dispute. The provision includes "condition precedent[s]" prohibiting Plaintiffs from initiating a lawsuit or arbitration unless notices include specific information outlined by Defendant and mandates a conference during the "Initial Dispute Resolution Period." This requires that Plaintiffs "personally appear at the conference," and "participate" regardless of whether they are represented by counsel.

167. Such language imposes new and significant hurdles for Plaintiffs to exercise their legal rights and to seek redress for the unauthorized disclosures of their highly sensitive genetic information.

168. Defendant's new November 2023 arbitration language also materially changes the TOS to unfairly impact Plaintiffs' choice of counsel by imposing a two-tiered set of arbitration procedures for Plaintiffs. Pursuant to TOS § 5(c), arbitrations are administered by

[19] Though 23andMe's counsel has indicated that the company does not intend to enforce the arbitration clause, he has yet to respond to the undersigned's request for a formal stipulation to that effect. To the extent a formal stipulation is provided, Plaintiffs will voluntarily dismiss this claim.

JAMS, unless they are subject to an exemption for "Mass Arbitration" defined as "25 more demands for arbitration . . . relating to the same or similar subject matter and sharing common issues of law or fact, and counsel for the parties submitting the demands are the same or coordinated." TOS § 5(c)(v). Unlike singular arbitrations, Mass Arbitrations are administered by NAM and are subject to the appointment and sole discretion of a "Procedural Arbitrator" with broad authority to "rule on proposals by the parties for the efficient and cost-effective management of the Mass Arbitration to the extent the parties cannot agree." TOS § 5(c)(v)(1). Such authority is not clearly defined in either Defendant's arbitration clause nor the relevant NAM rules and should be considered vague and standardless.

169. These terms will have an immediate impact on Defendant's customers' ability to obtain representation as plaintiffs' counsel will be deterred from representing more than the twenty-five-client threshold while the Defendant retains all advantages of a repeat-player—including the retention of the same law firm—in any dispute.

170. The surprise amendments to the TOS also deny Plaintiffs arbitrator selection rights articulated by California state law. *See* Cal. Civ. Proc. Code §§ 1281.9, 1281.91(b). NAM rules incorporated by the Defendant's language, allow for NAM to decide in Mass Arbitration, among other things, whether a challenged arbitrator is removed, the admissibility and the merits of a challenge, and for the appointment of the same arbitrator to multiple matters. *See* NAM Rule 23; NAM Mass Filing Rule 8. Such provisions run counter to statutory and unwaivable arbitrator selection rights under state law.

171. Defendant's amended arbitration clause further imposes a one-year contractual limitations period under TOS § 5(f) stating, "you agree that regardless of any statute or law to the contrary, any claim or cause of action arising out of or related to use of the Services or the Terms must be filed within one (1) year after such claim or cause of action arose or be forever barred." This provision unfairly imposes a period of limitations that is shorter than otherwise available under state law, including claims for negligence and unfair business practices pursuant to Cal. Bus. & Prof. Code § 17208.

172. Actual harm has arisen in the wake of the data breach and the unlawful

disclosure of Plaintiffs' genetic information. Since the data breach, Defendant has failed to provide sufficient details related to its scope and severity and to inform customers as to whether vulnerabilities in its systems, protocols, and practices have been remedied to prevent further exposure. As such, Defendant seeks to limit Plaintiffs' and Class Members' access to justice while they remain at imminent risk of continued exposure of their genetic information.

173. Pursuant to its authority under the Declaratory Judgment Act, this Court should enter a judgment, declaring, among other things, that:

(a) 23andMe continues to owe a legal duty and contractual obligations to Plaintiffs and Class Members; and

(b) The provisions in 23andMe's modified arbitration agreement, including the mandates for individual participation in dispute resolution proceedings, vague and standardless Mass Arbitration procedures, denials of arbitration selection rights protected by state law, and unreasonably time-constrained limitations periods are unconscionable, invalid, and unenforceable.

PRAYER FOR RELIEF

WHEREFORE, Plaintiffs Melvin and J.L., individually and on behalf of the Nationwide Class, the Vulnerable Persons Subclass, and the State Genetic Privacy Statute Subclass, respectfully request that this Court enter an Order:

(a) Certifying the Classes as defined above, appointing Plaintiffs Melvin and J.L. as the representatives of the Classes, and appointing their counsel as Class Counsel;

(b) Awarding injunctive relief requiring Defendant to take appropriate measures to strengthen the data security systems that maintain PGI and to prohibit Defendant from continuing to engage in the unlawful acts, omissions and practices described herein;

(c) Requiring Defendant to pay all costs associated with class notice and administration of class-wide relief;

(d) Awarding to Plaintiffs and all Class Members actual, compensatory,

consequential, incidental, nominal, and statutory damages, punitive damages, restitution and disgorgement in an amount to be determined at trial;

(e) Awarding injunctive relief requiring Defendant to: (i) strengthen its data security systems and monitoring procedures; (ii) submit to future annual audits of those systems and monitoring procedures; and (iii) provide notice to all impacted customers of the actual scope and severity of the breach, and informing them that their PGI has been leaked on the dark web, and with respect to the Vulnerable Persons Subclass members, informing them that they have been specifically targeted by the hacker;

(f) Establishing a TAM Fund for the benefit of the Vulnerable Persons Subclass that is sufficiently funded to provide the services described above for a period of twenty (20) years from the establishment date;

(g) Declaring on behalf of the State Genetic Privacy Statute Subclass that Defendant's conduct described herein violates the genetic privacy statutes identified herein;

(h) Declaring that Defendant's November 30, 2023 modifications to the TOS are void and unenforceable;

(i) Awarding the State Genetic Privacy Statute Subclass statutory damages as provided by each statute;

(j) Requiring Defendant to pay pre-judgment and post-judgment interest, as provided by law;

(k) Enjoining Defendant from further deceptive and unfair practices and making untrue statements with respect to the data breach and stolen PGI;

(l) Awarding equitable relief requiring restitution and disgorgement of the revenues wrongfully retained as a result of Defendant's wrongful conduct;

(m) Awarding reasonable attorneys' fees and costs; and

(n) Awarding such further relief that the Court deems reasonable and just.

JURY DEMAND

Plaintiffs request a trial by jury of all claims that can be so tried.

Respectfully Submitted,

DAVID MELVIN and J.L., individually and on behalf of all others similarly situated,

Dated: January 26, 2024

By: /s *Rafey S. Balabanian*
One of Plaintiffs' Attorneys

Rafey S. Balabanian (SBN 315962)
rbalabanian@edelson.com
EDELSON PC
150 California Street, 18th Floor
San Francisco, California 94111
Tel: 415.212.9300
Fax: 415.373.9435

Jay Edelson (*pro hac vice* forthcoming)
jedelson@edelson.com
J. Eli Wade-Scott (*pro hac vice* forthcoming)
ewadescott@edelson.com
Michael Ovca (*pro hac vice* forthcoming)
movca@edelson.com
Emily Penkowski Perez (*pro hac vice* forthcoming)
epenkowski@edelson.com
Hannah P. Hilligoss (*pro hac vice* forthcoming)
hhilligoss@edelson.com
EDELSON PC
350 North LaSalle Street, 14th Floor
Chicago, Illinois 60654
Tel: 312.589.6370
Fax: 312.589.6378

Counsel for Plaintiffs and the Putative Classes